Symantec Endpoint Protection Small Business Edition

Service Description

April 2015

Service Overview

The Symantec Endpoint Protection Small Business Edition ("*SEP SBE*") Service is an endpoint threat protection service that lets Customers choose a cloud-managed service or on-premise deployment option. This Service Description applies to the cloud-managed deployment option only. The on-premise option is governed by the Subscription Instrument and accompanying EULA.

This Service Description, with any attachments included by reference, is part of any agreement which incorporates this Service Description by reference (collectively, the "Agreement"), for those Services which are described in this Service Description and are provided by Symantec.

Table of Contents

TECHNICAL/BUSINESS FUNCTIONALITY AND CAPABILITIES
Service Features

- Customer can access the Service Management Console (SMC) by using a secure password protected login. The SMC provides the ability for Customer to configure and manage the Service, access reports, and view data and statistics when available as part of the Service.
- The Service is managed on a twenty-four (24) hours/day by seven (7) days/week basis and is monitored for hardware availability, service capacity and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- Reporting for the Service is available through the SMC. Reporting may include activity logs and/or statistics. Customer may choose to generate reports, through the SMC, which can be configured to be sent by Email on a scheduled basis, or downloaded from the SMC.
- During the Term, all logs and reports based on data reported by the agent are stored on, viewable and downloadable from the SMC for ninety (90) days, and will be automatically deleted at the end of that ninety (90) day period.
- The Service is intended to enable Customer to implement a valid and enforceable computer use policy, or its equivalent.
- Suggested word lists and template rules or policies supplied by Symantec contain words which may be considered offensive.
- In the event that continued provision of the Service to Customer would compromise the security of the Service, including, but not limited to, hacking attempts, denial of service attacks, mail bombs or other malicious activities either directed at or originating from Customer’s domains, Customer agrees that Symantec may temporarily suspend Service to Customer. In such an event, Symantec will promptly inform Customer and will work with Customer to resolve such issues. Symantec will reinstate the Service upon removal of the security threat.
- Should a Service be suspended for any reason whatsoever, Symantec shall reverse all configuration changes made upon provisioning the Service and it shall be the responsibility of Customer to undertake all other necessary configuration changes if the Service is reinstated.
- Should a Service be terminated for any reason whatsoever, Customer’s account may remain open; however, Customer will no longer have access to the Service.
- The Service is intended to:
  - Protect the computer from detected malwares based on known methods.
  - Block known malicious attacks from the network on the computer.
  - Provide available anti-phishing functionality on the supported browsers which will block suspected phishing attacks.
  - Block or allow access from USB storage devices based on Customer configuration.
- Symantec will publish the current list of supported computer operating systems for the agent and supported browser for the SMC.
- Using the SMC, Security Policies can be created and modified. These policies are then applied to the groups with that policy and are pushed down to the endpoints within that group.
- Customer may designate any local update hosts through the SMC which acts as a single hub, receiving the updated software and distributing it among the endpoints. This optional procedure reduces the required Internet traffic.

- Customer may configure the Service to send an automatic notification to configured Email recipients based on the alerts rule, configurable in the SMC. Notifications can be created, deleted and customized through the SMC.

Customer Responsibilities

Symantec can only perform the Service if Customer provides required information or performs required actions. If Customer does not provide/perform per the following responsibilities, Symantec's performance of the Service may be delayed, impaired or prevented, and/or eligibility for Service Level Agreement benefits may be voided, as noted below.

- Setup Enablement: Customer must provide information required for Symantec to begin providing the Service.
- Adequate Customer Personnel: Customer must provide adequate personnel to assist Symantec in delivery of the Service, upon reasonable request by Symantec.
- Renewal Credentials: If applicable, Customer must apply renewal credential(s) provided in the Subscription Instrument within its account administration, to continue to receive the Service, or to maintain account information and Customer data which is available during the Service Term.
- Customer Configurations vs. Default Settings: Customer must configure the features of the Service through the SMC, if applicable, or default settings will apply. In some cases, default settings do not exist and no Service will be provided until Customer chooses a setting. Configuration and use of the Service(s) are entirely in Customer's control.
- Installation of a Service Software is required for each affected end–user computer receiving the Service.
- Customer must manage the Service Software through the SMC.
- Customer must manage computers, policies, alerts and reports and other configuration options through the SMC.-
- Customer must make any required firewall changes to allow the agent to communicate and operate with the Service.

Supported Platforms and Technical Requirements

Supported platforms for the Service are defined at: http://www.symantec.com/endpoint-protection-small-business-edition/system-requirements**Hosted Service Software Components**

The Service includes the following software Service Components, upon payment of the applicable fee: Platform Agent, Antivirus Agent

Assistance and Technical Support

Customer Assistance**.** Symantec will provide the following assistance a part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support**.** The following technical support ("Support") is included with the Service.

- Support available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of the Service features and to resolve reported problems with the Service.

Maintenance. Symantec must perform maintenance from time to time. The following applies to such maintenance:

- *Planned Maintenance*. For Planned Maintenance, Symantec will use commercially reasonable efforts to give Customer seven (7) calendar days' notification, via email, SMS, or as posted on the SMC. Symantec will use commercially reasonable efforts to perform Planned Maintenance at times when collective customer activity is low, in the time zone in which the affected Infrastructure is located, and only on part, not all, of the network. If possible, Planned Maintenance will be carried out without affecting the Service. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance in order to minimize disruption of the Service. "**Planned Maintenance**" means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure.

- *Emergency Maintenance.* Where Emergency Maintenance is necessary and is likely to affect the Service, Symantec will endeavor to inform the affected parties in advance by posting an alert on the applicable SMC no less than one (1) hour prior to the start of the Emergency Maintenance. "**Emergency Maintenance**" means unscheduled maintenance periods which during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure or any maintenance for which Symantec could not have reasonably prepared for the need for such maintenance, and failure to perform the maintenance would adversely impact Customer.

- *Routine Maintenance (SMC).* Symantec will use commercially reasonable efforts to perform routine maintenance of SMCs at times when collective Customer activity is low to minimize disruption to the availability of the SMC. Customer will not receive prior notification for these routine maintenance activities.

SERVICE-SPECIFIC TERMS

Automatic Renewal Opt-Out Process

The Service renews automatically as set forth in the Agreement, unless Customer cancels as follows:

- Customer may opt-out of automatic renewal by providing Symantec notice, at least ninety (90) days prior to the end of Customer's Initial Period (also sometimes called the Minimum Period) or a then-current Renewal Period (each, a "Term").

- Such notice of automatic renewal opt-out, or notice of non-renewal, must be sent to the following address (or replacement address as published by Symantec): cloud_credit@symantec.com. A notice of non-renewal takes effect upon the expiration of the then-current Term. Any notice given according to this procedure will be deemed to have been given when received.

Service Conditions

- Customer may not disclose the results of any benchmark tests or other tests connected with the Service to any third party without Symantec's prior written consent.
- The use of any Service Component in the form of software shall be governed by the license agreement accompanying the software. If no EULA accompanies the Service Component, it shall be governed by the terms and conditions located at (http://www.symantec.com/content/en/us/enterprise/eulas/b-hosted-service-component-eula-eng.pdf). Any additional rights and obligations with respect to the use of such Service Component shall be as set forth in this Service Description.
- The use of any Service Component in the form of hardware shall be governed by the warranty card accompanying the hardware.
- Except as otherwise specified in the Service Description, the Service (including any Hosted Service Software Component provided therewith) may use open source and other third party materials that are subject to a separate license. Please see the applicable Third Party Notice, if applicable, at http://www.symantec.com/about/profile/policies/eulas/.

- Symantec may update the Service at any time in order to maintain the effectiveness of the Service.
- Instances: Notwithstanding anything to the contrary contained in this Service Description, each running instance (physical and/or virtual) of the Service Software must be licensed. An "instance" of Service Software is created by executing the Service Software's setup or install procedure. An "instance" of Service Software is created by duplicating an existing instance. References to the Service Software include "instances" of the Service Software. Customer "runs an instance" of software by loading it into memory and executing one or more of its instructions. Once running, an instance is considered to be running (whether or not its instructions continue to execute) until it is removed from memory.
- Terminal Servers: If the Service Software is for use on a hardware device/server that provides endpoints with a common connection point to a local or wide area network (a "Licensed Terminal Server"), and such Licensed Terminal Server(s) is/are accessed by endpoints that do not have installed copies of the Service Software ("Thin Clients"), then every Thin Client accessing a Licensed Terminal Server is considered an "instance" and must have a valid license to the Service Software. In the event that the Licensed Terminal Server(s) is/are accessed by endpoints which have authorized copies of the Service Software already installed ("Thick Clients"), such access of the Licensed Terminal Server(s) by Thick Clients shall not be considered additional "instances" and Customer is not required to purchase additional licenses to the Service Software.
- CUSTOMER ACKNOWLEDGES AND AGREES THAT PART OR ALL OF THE SERVICE MAY BE PERFORMED IN THE UNITED STATES OF AMERICA
- As indicated in the applicable Subscription Instrument, Customer may choose to deploy either the cloud-managed or on-premise option at any time during the applicable License Term, but not both at the same time. All Users of the Service, regardless of when the Service was purchased, must use the same deployment option. If Customer is changing from one deployment option to the other, Customer will have a grace period of sixty (60) calendar days to complete such change. If Customer chooses to deploy the on-premise option, Customer must upgrade to the most current version within ninety (90) calendar days of availability of such upgrade.
- When Customer is using the cloud-managed Service, Customer may deploy the on-premise option to protect an environment for which the cloud-managed Service is not yet available. Any deployment of the on-premise option must be included in the total User count. Customer will have sixty (60) calendar days to synchronize the deployment of all Users, once the cloud-managed Service becomes available for that environment.

Optional Feedback.

- The Service may contain a voluntary feedback feature that allows Customer to provide feedback regarding the Service. By providing such feedback, Customer grants to Symantec, under Customer's intellectual property rights, a worldwide, royalty-free, irrevocable and non-exclusive license, with the right to sublicense to Symantec's licensees and customers, the rights to use and disclose the feedback in any manner Symantec chooses and to display, perform, copy, make, have made, use, sell, and otherwise dispose of Symantec's and its sublicensee's products embodying such feedback in any manner and in any media Symantec or its sublicensees choose, without reference or obligation to Customer. Customer's use of the Service does not require Customer to provide any feedback and use of this feedback feature is entirely voluntary.

SERVICE LEVEL AGREEMENT

General

- If Customer believes it is entitled to a remedy in accordance with this Service Level Agreement, Customer must submit a Credit Request within ten (10) business days of the end of the calendar month in which the suspected service level noncompliance occurred. Customer recognizes that logs are only kept for a limited number of calendar days and therefore any Credit Request submitted outside of the provided timeframe will be deemed invalid.

- All Credit Requests will be subject to verification by Symantec in accordance with the applicable provisions of this Service Level Agreement.
- This Service Level Agreement will not operate: (i) during periods of Planned Maintenance or Emergency maintenance, periods of non-availability due to force majeure or acts or omissions of either Customer or a third party; (ii) during any period of suspension of service by Symantec in accordance with the terms of the Agreement or (iii) where Customer is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (iv) Customer has not configured the Service in accordance with the Agreement.
- The remedies set out in this Service Level Agreement shall be Customer's sole and exclusive remedy in contract, tort (including without limitation negligence) or otherwise, with respect to this Service Level Agreement.
- The maximum accumulative liability of Symantec under this Service Level Agreement in any calendar month shall be no more than one hundred percent (100%) of the Monthly Charge payable by Customer for the affected Service(s).

- The Service will be Available 100% of each calendar month, exclusive of Planned Maintenance and Emergency Maintenance windows. In this case, "Available" is defined as the Symantec hosted Infrastructure being ready to synchronize policy information. For the purposes of calculating non-availability the following criteria will apply: (i) the measurement will be performed by Symantec's monitoring systems (such measurement may be provided to Customer upon written request), (ii) only the Symantec hosted Infrastructure will be measured and such measurement excludes any non-availability as a result of a Customer network outage, a third party outage, or DNS issues outside of the direct control of Symantec.
- For each one (1) percent or part thereof of non-availability beyond the availability target of 100% in the calendar month in question, Customer will be entitled to a Service Credit equivalent to 10% of the Monthly Charges due to Symantec for the Service, subject to a maximum of 100% of the Monthly Charge. Customer may terminate the Service, at its sole option, if at any time this availability falls below 90% in any calendar month.

  The Service Credit described in this section shall be Customer's sole and exclusive remedy in connection with any unavailability of the Service.

24x7 Technical Support and Fault Response

- Symantec will on a twenty-four (24) hours/day by seven (7) days/week basis:
  - provide technical support to Customer for problems with the Service; and
  - liaise with Customer to resolve such problems.
- Whenever a Customer raises a problem, fault or request, for service information via telephone or Email with Symantec, its priority level is determined and it is responded to per the response targets defined in the table below:

Priority Level	Definition	Response Target	Percentage Credit of Monthly Charge for Failure to Meet Target
Severity 1	Loss of Service	95% of calls responded to within 2 hours	15
Severity 2	Partial loss of Service or Service impairment	85% of calls responded to within 4 hours	10

Severity 3	Potentially Service affecting or non-Service affecting information request	75% of calls responded to within 8 hours	5

- Faults originating from Customer's actions or requiring the actions of other service providers are beyond the control of Symantec and as such are specifically excluded from this Service Level.

- If Customer believes that it has experienced a delay in Symantec response to a request (outside the parameters of the Response Targets described above) it may be entitled to a Service Credit in accordance with the table above. Credit Requests must state the time, date and the log number of the incident.

DATA PRIVACY NOTICE

- The Service utilizes the LiveUpdate functionality. For the LiveUpdate functionality, please refer to the LiveUpdate privacy notice available at http://www.symantec.com/about/profile/policies/luprivacy.jsp.
- In order to promote awareness, detection and prevention of Internet security risks, Symantec may share the information collected through the Service with research organizations and other security software vendors. Symantec may also use statistics derived from the information collected through the Service or submitted by Customer to track and publish reports on security risk trends.

DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement or this Services Description, have the meaning given below:

- "**Administrator**" means a Customer User with authorization to manage the Service on behalf of Customer. Administrators may have the ability to manage all or part of a Service as designated by Customer.
- **"Credit Request"** means the notification which Customer must submit to Symantec by Email to support.cloud@symantec.com with the subject line "Credit Request" (unless otherwise notified by Symantec).
- "**Email**" means any inbound or outbound SMTP message passing through a Service.
- "**End User License Agreement (EULA)**" means the terms and conditions accompanying Software (defined below).
- "**Infrastructure**" means any Symantec or licensor technology and intellectual property used to provide the Services.
- **"Monthly Charge"** means the monthly charge for the affected Service(s) as defined in the Agreement.
- "**Service Component**" means certain enabling software, hardware peripherals and associated documentation which may be separately provided by Symantec as an incidental part of a Service.
- "**Service Credit**" means the amount of money that will be credited to Customer's next invoice after submission of a Credit Request and validation by Symantec that a credit is due to Customer.

- "**Service Software**" means Software (defined below), as may be required by a Service, which must be installed on each Customer computer, in order to receive the Service. Service Software includes the Software and associated documentation that may be separately provided by Symantec as part of the Service.
- "**Software**" means each Symantec or licensor software program, in object code format, licensed to Customer by Symantec and governed by the terms of the accompanying EULA, or this Service Description, as applicable, including without limitation new releases or updates as provided hereunder.
- "**Subscription Instrument**" means one or more of the following applicable documents which further defines Customer's rights and obligation related to the Service: a Symantec certificate or a similar document issued by Symantec, or a written agreement between Customer and Symantec, that accompanies, precedes or follows the Service.
- "**User**" means an individual person and/or device authorized to use and/or benefits from the use of the Service, or that actually uses any portion of the Service. For the Email Security Services and/or Email Archiving Services, the definition of "**User**" shall include all mailboxes that send and/or receive Email.

END OF SERVICE DESCRIPTION